INTERFERENCE SEARCH

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	1	(prime number private public key generator random identities equality).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/18 20:54
L3	1	(prime number private public key generator random verifier equality).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/18 20:54
L4	1	(prime number private public key security parameter prover verifier).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/18 20:54
L5	1	(authenticat$3 identities public$3 uniformly non-negative).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/18 20:55

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1236	(380/30).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/18 20:56
L2	1342	(380/28).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/18 20:56
L3	1666	(713/168).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/18 20:56
L4	3889	L2 L3 L1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 20:56
L5	3107	L4 and @ad<"20030826"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 21:59
L7	625	L5 and (prime near2 number)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 20:58
L8	357	L7 and ((private near2 key) and (public near2 key))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 21:05
L9	779	(380/270).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/18 21:05
L10	557	L9 and @ad<"20030826"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 22:20

EAST Search History

L11	3580	L10 or L5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 22:05
L13	163	L11 and (zero near2 knowledge)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 22:19
L14	30	L13 and prover and verifier and (prime near2 number)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 22:20
L16	20	L14 and (private near2 key) and (public near2 key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 22:32
L17	1	L16 and equality	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 22:27
L18	2	("4995082").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/18 22:27
L20	4	L16 and optical	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 22:32
L21	8	(prime adj number) same identit$3 same (private adj key) same (public adj key) same generator	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 22:55
L23	1	("2005/0058288").URPN.	USPAT	OR	ON	2007/03/18 22:57
L24	3	authenticat$3 same identit$3 same parallel same prover same verifier	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 23:01

EAST Search History

L25	3	identit$3 same parallel same prover same verifier	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 23:01
L26	4	parallel same prover same verifier	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 23:04
L28	185	prover same verifier	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 23:04
L29	140	L28 and @ad<"20030826"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 23:04
L30	27	L29 and (public adj key) and (private adj key) and (prime adj number)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/18 23:05
S1	90	(("(20050058288") or ("5581615") or ("7184547") or ("6078909") or ("6011848") or ("6044463") or ("20010044895") or ("20040123156") or ("20030203756") or ("20040117630") or ("6889322") or ("6978372") or ("20040111617") or ("20060112273") or ("6154841") or ("20050278536") or ("20060195692") or ("6962530") or ("20030115464") or ("20040133781") or ("20050220298") or ("6829356") or ("7047408") or ("5245657") or ("6058476") or ("6301660") or ("5345506") or ("20040073795") or ("5963649") or ("6076163") or ("5761309") or ("6952476") or ("20050114662") or ("20050265550") or ("4932056") or ("6320966") or ("6937728") or ("6108783") or ("6226383") or ("6226383") or ("5590199") or ("6216231") or ("6216231") or ("6256741") or ("5757918") or ("6327659") or ("6332192") or ("20010005887") or ("7174459") or ("20050005119") or (").pn.")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/18 20:56
S2	1236	(380/30).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/15 15:03
S3	1342	(380/28).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/15 15:21

EAST Search History

S4	1666	(713/168).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/15 15:21

Terms used
zero and **knowledge** and **prime** and **number** and **private** and **public** and **key** and **prover** and **verifier** and **equal**

Sort results by relevance
Display results expanded form

Save results to a Binder
Search Tips
☐ Open results in a new window

Try an Advanced Search
Try this search in The ACM Gui

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 Some facets of complexity theory and cryptography: A five-lecture tutorial

Jörg Rothe
December 2002 **ACM Computing Surveys (CSUR)**, Volume 34 Issue 4
Publisher: ACM Press

Full text available: pdf(2.78 MB) Additional Information: full citation, abstract, references, citings, index terms review

In this tutorial, selected topics of cryptology and of computational complexity theory are presen We give a brief overview of the history and the foundations of classical cryptography, and then on to modern public-key cryptography. Particular attention is paid to cryptographic protocols an problem of constructing key components of protocols such as one-way functions. A function is o way if it is easy to compute, but hard to invert. We discuss the notion of one-way functions botl

Keywords: Complexity theory, interactive proof systems, one-way functions, public-key cryptography, zero-knowledge protocols

2 On randomization in sequential and distributed algorithms

Rajiv Gupta, Scott A. Smolka, Shaji Bhaskar
March 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 1
Publisher: ACM Press

Full text available: pdf(8.01 MB) Additional Information: full citation, abstract, references, citings, index terms

Probabilistic, or randomized, algorithms are fast becoming as commonplace as conventional deterministic algorithms. This survey presents five techniques that have been widely used in the design of randomized algorithms. These techniques are illustrated using 12 randomized algorith both sequential and distributed— that span a wide range of applications, including: primality tes classical problem in number theory), interactive probabilistic proof s ...

Keywords: Byzantine agreement, CSP, analysis of algorithms, computational complexity, dinin philosophers problem, distributed algorithms, graph isomorphism, hashing, interactive probabili proof systems, leader election, message routing, nearest-neighbors problem, perfect hashing, primality testing, probabilistic techniques, randomized or probabilistic algorithms, randomized quicksort, sequential algorithms, transitive tournaments, universal hashing

3 Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proc

systems
Oded Goldreich, Silvio Micali, Avi Wigderson
July 1991 **Journal of the ACM (JACM)**, Volume 38 Issue 3
Publisher: ACM Press
Full text available: pdf(3.04 MB) Additional Information: full citation, references, citings, index terms

Keywords: NP, cryptographic protocols, fault tolerant distributed computing, graph isomorphis interactive proofs, methodological design of protocols, one-way functions, proof systems, zero-knowledge

4 Multiagent systems and electronic markets track: Practical secrecy-preserving, verifiably c and trustworthy auctions
D. C. Parkes, M. O. Rabin, S. M. Shieber, C. A. Thorpe
August 2006 **Proceedings of the 8th international conference on Electronic commerce: The e-commerce: innovations for conquering current barriers, obstacles and limit to conducting successful business on the internet ICEC '06**
Publisher: ACM Press
Full text available: pdf(507.45 KB) Additional Information: full citation, abstract, references

We present a practical system for conducting sealed-bid auctions that preserves the secrecy of bids while providing for verifiable correctness and trustworthiness of the auction. The auctionee accept all bids submitted and follow the published rules of the auction. No party receives any us information about bids before the auction closes and no bidder is able to change or repudiate he Our solution uses Paillier's homomorphic encryption scheme [25] for zero knowledge proofs of .

5 Authentication and integrity in outsourced databases
Einar Mykletun, Maithili Narasimha, Gene Tsudik
May 2006 **ACM Transactions on Storage (TOS)**, Volume 2 Issue 2
Publisher: ACM Press
Full text available: pdf(531.47 KB) Additional Information: full citation, abstract, references, index terms

In the Outsourced Database (ODB) model, entities outsource their data management needs to a third-party service provider. Such a service provider offers mechanisms for its clients to create, update, and access (query) their databases. This work provides mechanisms to ensure data inte and authenticity for outsourced databases. Specifically, this article provides mechanisms that as the querier that the query results have not been tampered with and are authentic (with respect the ...

Keywords: Outsourced databases, authentication, data authenticity, data integrity, integrity, signature aggregation, storage

6 Credentials: Direct anonymous attestation
Ernie Brickell, Jan Camenisch, Liqun Chen
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**
Publisher: ACM Press
Full text available: pdf(314.67 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper describes the direct anonymous attestation scheme (DAA). This scheme was adopte the Trusted Computing Group (TCG) as the method for remote authentication of a hardware mo called Trusted Platform Module (TPM), while preserving the privacy of the user of the platform t contains the module. DAA can be seen as a group signature without the feature that a signature be opened, i.e., the anonymity is not revocable. Moreover, DAA allows for pseudonyms, i.e., for

signat ...

Keywords: anonymous credential systems, cryptographic protocols, integrity based computing privacy, trusted computing

7 Practical multi-candidate election system

Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, Guillaume Poupard
August 2001 **Proceedings of the twentieth annual ACM symposium on Principles of distribu computing PODC '01**
Publisher: ACM Press
Full text available: pdf(898.50 KB) Additional Information: full citation, abstract, references, citings, index terms

The aim of electronic voting schemes is to provide a set of protocols that allow voters to cast ba while a group of authorities collect the votes and output the final tally. In this paper we describe practical multi-candidate election scheme that guarantees privacy of voters, public verifiability, robustness against a coalition of malicious authorities. Furthermore, we address the problem of receipt-freeness and incoercibility of voters. Our new scheme is based on the Paillier cryp ...

8 Zero knowledge proofs of identity

U. Fiege, A. Fiat, A. Shamir
January 1987 **Proceedings of the nineteenth annual ACM conference on Theory of computir STOC '87**
Publisher: ACM Press
Full text available: pdf(995.58 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper we extend the notion of zero knowledge proofs of membership (which reveal one b information) to zero knowledge proofs of knowledge (which reveal no information whatsoever). formally defining this notion, we show its relevance to identification schemes, in which parties p their identity by demonstrating their knowledge rather than by proving the validity of assertions describe a novel scheme which is provably secure if factoring is difficult and whose practic ...

9 Efficient verifiable encryption (and fair exchange) of digital signatures

Giuseppe Ateniese
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**
Publisher: ACM Press
Full text available: pdf(781.40 KB) Additional Information: full citation, abstract, references, citings, index terms

A fair exchange protocol allows two users to exchange items so that either each user gets the o item or neither user does. In [2], verifiable encryption is introduced as a primitive that can be u build extremely efficient fair exchange protocols where the items exchanged represent digital signatures. Such protocols may be used to digitally sign contracts.This paper presents new simp schemes for verifiable encryption of digital signatures. We make us ...

Keywords: contract signing problem, digital signatures, fair exchange, proof of knowledge, pul key cryptography, verifiable encryption

10 Privacy and anonymity: Applications of secure electronic voting to automated privacy-pres troubleshooting

Qiang Huang, David Jao, Helen J. Wang
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press
Full text available: pdf(237.64 KB) Additional Information: full citation, abstract, references, index terms

Recent work [27, 15] introduced a novel peer-to-peer application that leverages content sharin aggregation among the peers to diagnose misconfigurations on a desktop PC. This application p interesting challenges in preserving privacy of user configuration data and in maintaining integr troubleshooting results. In this paper, we provide a much more rigorous cryptographic and yet practical solution for preserving privacy, and we investigate and analyze solutions for ensuring integri ...

Keywords: automatic troubleshooting, homomorphic encryption, integrity, privacy, zero knowl proof

11 Emerging applications: Almost entirely correct mixing with applications to voting

Dan Boneh, Philippe Golle
November 2002 **Proceedings of the 9th ACM conference on Computer and communications security CCS '02**
Publisher: ACM Press
Full text available: pdf(199.48 KB) Additional Information: full citation, abstract, references, citings, index terms

In order to design an exceptionally efficient mix network, both asymptotically and in real terms, develop the notion of almost entirely correct mixing, and propose a new mix network that is aln entirely correct. In our new mix, the real cost of proving correctness is orders of magnitude fast than all other mix nets. The trade-off is that our mix only guarantees "almost entirely correct" r i.e it guarantees that the mix network processed correctly all inputs with high (but not overw ...

Keywords: electronic voting, mix networks

12 Concurrent zero-knowledge

Cynthia Dwork, Moni Naor, Amit Sahai
November 2004 **Journal of the ACM (JACM)**, Volume 51 Issue 6
Publisher: ACM Press
Full text available: pdf(316.80 KB) Additional Information: full citation, abstract, references, citings, index terms

Concurrent executions of a zero-knowledge protocol by a single prover (with one or more verifie may leak information and may not be zero-knowledge *in toto*. In this article, we study the probl maintaining zero-knowledge.We introduce the notion of an (α, β) *timing constraint*: for any two processors P_1 and P_2, if P_1 measures α elapsed time on its local clock and P_2 measures β elapse

Keywords: Zero knowledge, composition, cryptographic protocols

13 Verifiable encryption of digital signatures and applications

Giuseppe Ateniese
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issu
Publisher: ACM Press
Full text available: pdf(258.12 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a new simple schemes for verifiable encryption of digital signatures. We ma use of a trusted third party (TTP) but in an *optimistic* sense, that is, the TTP takes part in the pr only if one user cheats or simply crashes. Our schemes can be used as primitives to build efficie exchange and certified e-mail protocols.

Keywords: Certified e-mail, contract signing, digital signatures, fair exchange, proof of knowle public-key cryptography

14 Protocols: A verifiable secret shuffle and its application to e-voting

C. Andrew Neff

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**

Publisher: ACM Press

Full text available: pdf(216.76 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a mathematical construct which provides a cryptographic protocol to *verifiably shuffl* sequence of *k* modular integers, and discuss its application to secure, universally verifiable, mul authority election schemes. The output of the shuffle operation is another sequence of *k* modula integers, each of which is the same secret power of a corresponding input element, but the orde elements in the output is kept secret. Though it is a trivial matter for the "shu ...

Keywords: anonymous credentials, electronic voting, honest-verifier, mix-net, permutation, universal verifiability, verifiable mix, verifiable shuffle, zeroknowledge

15 Credentials: Group signatures with verifier-local revocation

Dan Boneh, Hovav Shacham

October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**

Publisher: ACM Press

Full text available: pdf(250.40 KB) Additional Information: full citation, abstract, references, index terms

Group signatures have recently become important for enabling privacy-preserving attestation in projects such as Microsoft's ngscb effort (formerly Palladium). Revocation is critical to the secur such systems. We construct a short group signature scheme that supports Verifier-Local Revoca (VLR). In this model, revocation messages are only sent to signature verifiers (as opposed to bo signers and verifiers). Consequently there is no need to contact individual signers when some u

Keywords: group signatures, revocation, trusted computing

16 Knowledge on the average—perfect, statistical and logarithmic

William Aiello, Mihir Bellare, Ramarathnam Venkatesan

May 1995 **Proceedings of the twenty-seventh annual ACM symposium on Theory of comp STOC '95**

Publisher: ACM Press

Full text available: pdf(1.18 MB) Additional Information: full citation, references, citings, index terms

17 Short papers: Anonymous yet accountable access control

Michael Backes, Jan Camenisch, Dieter Sommer

November 2005 **Proceedings of the 2005 ACM workshop on Privacy in the electronic society WPES '05**

Publisher: ACM Press

Full text available: pdf(178.78 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper introduces a novel approach for augmenting attribute-based access control systems way that allows them to offer fully anonymous access to resources while at the same time achie strong accountability guarantees. We assume that users hold attribute certificates and we show to exploit cryptographic zero-knowledge proofs to allow requesting users to prove that they hol suitable certificates for accessing a resource. In contrast to the commonly taken approach of se all p ...

Keywords: access control, accountability, anonymous credentials, anonymous transactions,

certificates, privacy

18 Verifiable partial key escrow

Mihir Bellare, Shafi Goldwasser

April 1997 **Proceedings of the 4th ACM conference on Computer and communications sec CCS '97**

Publisher: ACM Press

Full text available: pdf(1.98 MB) Additional Information: full citation, references, citings, index terms

19 On the limits of non-approximability of lattice problems

Oded Goldreich, Shafi Goldwasser

May 1998 **Proceedings of the thirtieth annual ACM symposium on Theory of computing S '98**

Publisher: ACM Press

Full text available: pdf(1.18 MB) Additional Information: full citation, references, citings, index terms

20 Resettable zero-knowledge (extended abstract)

Ran Canetti, Oded Goldreich, Shafi Goldwasser, Silvio Micali

May 2000 **Proceedings of the thirty-second annual ACM symposium on Theory of comput STOC '00**

Publisher: ACM Press

Full text available: pdf(1.21 MB) Additional Information: full citation, references, citings, index terms

Keywords: concurrent zero-knowledge, identification schemes, public-key cryptography, smart cards, witness-indistinguisable proofs, zero-knowledge

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next